Wykorzystanie norm w projektowaniu i utrzymywaniu systemów informatycznych służących do przetwarzania danych osobowych

Andrzej Kaczmarek
Biuro
Generalnego Inspektora
Ochrony Danych Osobowych

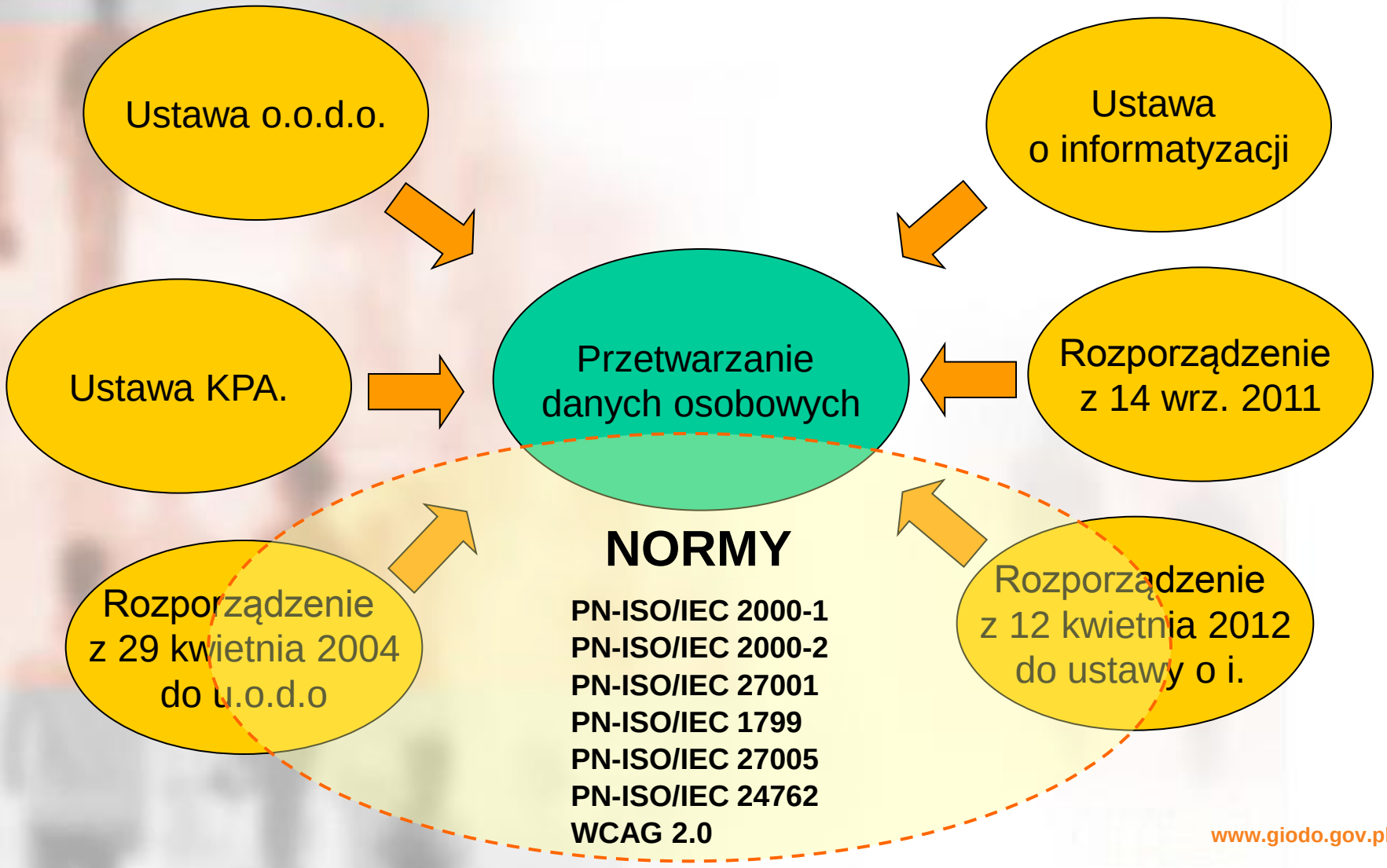
05. 2009 r. Wars

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

PLAN

- Główne elementy ochrony danych osobowych
- Ustawy i rozporządzenia jako główne źródło przepisów prawa
- Bezpieczeństwo informacji, ochrona danych – jako zagadnienia ogólne i specjalistyczne.
- Co dają standardy i jak można je wykorzystać.
- Standardy jako uzupełnienie przepisów prawa

GŁÓWNE OBSZARY REGULACJI W ZAKRESI OCHRONY DANYCH OSOBOWYCH



www.giodo.gov.pl

OCHRONA DANYCH OSOBOWYCH - DEFINICJE (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Definicje: Dane osobowe

1. Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

OCHRONA DANYCH OSOBOWYCH - DEFINICJE (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Definicje: zbiór danych, przetwarzanie

1. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
2. Przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

ZASADY PRZETWARZANIA DANYCH - PRZEPISY PRAWA (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zasady przetwarzania – Przetwarzanie danych jest dopuszczalne tylko wtedy gdy:

1. Osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,
2. Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
3. Jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie tej osoby,
4. Jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
5. jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

ZASADY PRZETWARZANIA DANYCH - PRZEPISY PRAWA (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki ADO – obowiązek informacyjny

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. Adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,
2. Celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,
3. Prawie dostępu do treści swoich danych oraz ich poprawiania,
4. Dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

ZASADY PRZETWARZANIA DANYCH - PRZEPISY PRAWA (3)

Obowiązki ADO – zapewnienie ochrony interesów osób, których dane dotyczą poprzez zapewnie nie, aby dane były:

1. Przetwarzane zgodnie z prawem;
2. Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi;
3. Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4. Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

ZASADY PRZETWARZANIA DANYCH - PRZEPISY PRAWA (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki ADO – obowiązek zgłoszenia zbioru do rejestracji.

1. Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi, z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. u.o.d.o (art. 40)
2. Z obowiązku rejestracji zbioru danych zwolnieni są administratorzy danych: (art. 43 ust. 1 u.o.d.o)
   - zawierających informacje niejawne;
   - ……
   - przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się;
   - ……

www.giodo.gov.pl

OBOWIĄZEK ZABEZPIECZENIA DANYCH OSOBOWYCH (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo – Obowiązek zabezpieczenia danych

Art. 36 u.o.d.o.)

1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

OBOWIĄZEK ZABEZPIECZENIA DANYCH OSOBOWYCH (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo – Obowiązek zabezpieczenia danych

Art. 39a.

Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

PRZYKŁADY ZBIORÓW DANYCH PRZETWARZANYCH W SZKOLE (1)

- Księga Ewidencji Dzieci w Szkole Podstawowej (coroczna adnotacja o spełnianiu przez dziecko obowiązku szkolnego)
- Zbiór uczniów szkoły (dane w różnych miejscach: Karta zapisu dziecka do szkoły, Księga Ewidencji Uczniów, Dziennik lekcyjny, Arkusz Ocen, Ewidencja legitymacji szkolnych, dane przetwarzane przez pedagoga)
- Zbiór danych osób korzystających z biblioteki szkolnej
- Zbiór ewidencja wejść do placówki
- Zbiór danych rodziców/opiekunów prawnych uczniów

PRZYKŁADY ZBIORÓW DANYCH PRZETWARZANYCH W SZKOLE (2)

- Zbiór danych kadrowo – płacowych
- Zbiór kandydatów do pracy
- Zbiór skarg i wniosków
- Zbiór rejestr korespondencji

NAJWAŻNIEJSZE PRZEPISY DOTYCZĄCE PRZETWARZANIE DANYCH W SZKOLE

- Ustawa z dnia 7 września 1991 r. o systemie oświaty (t.j.: Dz. U. 2004 r. Nr 256 poz. 2572)
- Ustawa z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz.U.2011.139.814)
- Rozporządzenie MEN z dn. 29.08.2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz.U. z 2014 r. poz. 1170) zastąpiło rozp. MENiS z dn. 19.02.2002 r.
- Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (t.j.: Dz. U. 2014 r. poz. 382)
- Ustawa z dnia 26 czerwca 1974 r. kodeks pracy

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie księgi ewidencji dzieci podlegających obowiązkowi szkolnemu (§ 4 Rozporządzenia w spr. dok.)

Do księgi ewidencji dzieci wpisuje się:

1) według roku urodzenia: imię (imiona) i nazwisko, datę i miejsce urodzenia, **numer PESEL** oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców oraz adresy ich zamieszkania, jeżeli są różne od adresu zamieszkania dziecka;
2) informacje o:
   a) przedszkolu lub innej formie wychowania przedszkolnego,
   b) Spełnianiu obowiązku rocznego przygotowania przedszkolnego
   c) odroczeniu rozpoczęcia obowiązku szkolnego,
   d) szkole, w której dziecko spełnia obowiązek szkolny,
   e) Spełnianiu obowiązku szkolnego poza szkołą.

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (2)

Prowadzenie księgę ewidencji dzieci będących absolwentami szkoły podstawowej, podlegających obowiązkowi szkolnemu, zamieszkałych w obwodzie gimnazjum. (§ 5 Rozporządzenia w spr. dok.)

Do księgi ewidencji dzieci podlegających obowiązkowi szkolnemu, zamieszkałych w obwodzie gimnazjum wpisuje się:

1) według roku urodzenia: imię (imiona) i nazwisko, datę i miejsce urodzenia, **numer PESEL** oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców oraz adresy ich zamieszkania, jeżeli są różne od adresu zamieszkania dziecka;
2) informacje o:
   a) szkole, w której dziecko spełnia obowiązek szkolny,
   b) spełnianiu przez dziecko obowiązku szkolnego poza szkołą, ze wskazaniem zezwolenia dyrektora gimnazjum, na podstawie którego dziecko spełnia obowiązek szkolny poza szkołą.

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie księgi uczniów (§ 6 Rozporządzenia w spr. dok.)

- Do księgi uczniów wpisuje się imię (imiona) i nazwisko, datę i miejsce urodzenia, **numer PESEL** oraz adres zamieszkania ucznia, imiona i nazwiska rodziców oraz adresy ich zamieszkania, jeżeli są różne od adresu zamieszkania ucznia, a także datę rozpoczęcia nauki w danej szkole oraz oddział, do którego ucznia przyjęto. W księdze uczniów odnotowuje się datę ukończenia szkoły albo datę i przyczynę opuszczenia szkoły przez ucznia.
- Wpisów w księdze uczniów dokonuje się chronologicznie według dat rozpoczęcia nauki w danej szkole.
- Szkoła dla dorosłych prowadzi księgę słuchaczy. Przepisy ust. 2 i 3 stosuje się odpowiednio.
- Do księgi uczniów albo słuchaczy prowadzonej odpowiednio przez szkołę policealną dla młodzieży lub szkołę dla dorosłych nie wpisuje się danych rodziców pełnoletnich uczniów albo słuchaczy.

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie dziennika lekcyjnego (§ 10 Rozporządzenia ….)

1) Szkoła prowadzi dla każdego oddziału dziennik lekcyjny, w którym dokumentuje się przebieg nauczania w danym roku szkolnym.
2) Do dziennika lekcyjnego wpisuje się w porządku alfabetycznym lub innym ustalonym przez dyrektora szkoły :
   - nazwiska i imiona uczniów albo słuchaczy, daty i miejsca urodzenia oraz adresy ich zamieszkania, imiona i nazwiska rodziców oraz adresy ich zamieszkania, jeżeli są różne od adresu zamieszkania ucznia albo słuchacza, adresy poczty elektronicznej rodziców i numery ich telefonów, jeżeli je posiadają, imiona i nazwiska nauczycieli prowadzących zajęcia edukacyjne oraz tygodniowy plan zajęć edukacyjnych, a w szkołach dla dorosłych prowadzących kształcenie w formie zaocznej - semestralny plan zajęć edukacyjnych. W przypadku dziennika lekcyjnego prowadzonego przez szkołę policealną dla młodzieży lub przez szkołę dla dorosłych nie wpisuje się danych dotyczących rodziców pełnoletnich uczniów lub słuchaczy
   - obecność, oceny, tematy zajęć…

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie dzienników w formie elektronicznej (§ 22)

1. Dzienniki, o których mowa w § 3, 10-14, 19 i 21, mogą być prowadzone także w formie elektronicznej.
2. Za zgodą organu prowadzącego, dzienniki, o których mowa w § 3, 10-14, 19 i 21, mogą być prowadzone wyłącznie w formie elektronicznej.
3. Prowadzenie dziennika elektronicznego wymaga:
   1) zachowania selektywności dostępu do danych;
   2) zabezpieczenia danych przed dostępem osób nieuprawnionych;
   3) zabezpieczenia danych przed zniszczeniem, uszkodzeniem lub utratą;
   4) rejestrowania historii zmian i ich autorów;
   5) umożliwienia bezpłatnego wglądu rodzicom w zakresie dotyczącym ich dzieci.

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (5)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie dzienników w formie elektronicznej (§ 22) c.d.

4. System informatyczny służący do prowadzenia dzienników elektronicznych powinien umożliwiać eksport danych do formatu **XML** oraz sporządzenie w formie papierowej dzienników, o których mowa w § 3, 10-14, 19 i 21.

5. W przypadku prowadzenia dzienników, o których mowa w § 3, 10, 11, 13 i 21, wyłącznie w formie elektronicznej, wpisanie przez nauczyciela w dzienniku elektronicznym tematu zajęć, o których mowa w § 3 ust. 2, § 10 ust. 3 i 5, § 11 ust. 2, § 13 ust. 3 i 5 oraz § 21 ust. 2 i 3, jest równoznaczne z potwierdzeniem przez nauczyciela przeprowadzenia tych zajęć.

PRZYKŁADY STOSOWANIA PRZEPISÓW SZCZEÓŁOWYCH W SZKOLE (6)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zabezpieczenie dzienników elektronicznych (§ 23)

W terminie 10 dni od dnia zakończenia roku szkolnego, a w przypadku szkół policealnych dla młodzieży oraz szkół dla dorosłych - w terminie 10 dni od dnia zakończenia semestru, dane stanowiące dziennik elektroniczny zapisuje się na informatycznym nośniku danych, według stanu odpowiednio na dzień zakończenia roku szkolnego oraz na dzień zakończenia semestru, w sposób zapewniający możliwość:

1) sprawdzenia integralności danych przez zastosowanie podpisu elektronicznego, o którym mowa w art. 3 pkt 1 ustawy o podpisie elektronicznym;
2) weryfikacji podpisu elektronicznego lub danych identyfikujących;
3) odczytania danych stanowiących dziennik elektroniczny w okresie przewidzianym dla przechowywania dzienników, o których mowa w § 3, 10-14, 19 i 21.

WYMAGANIA BEZPIECZEŃSTWA W ZAKRESIE OCHRONY DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024)

www.giodo.gov.pl

WYMAGANIA W ZAKRESIE DOKUMENTACJI PRZETWARZANIA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki administratora danych osobowych w zakresie dokumentacji przetwarzania danych osobowych ?

Dokumentacja przetwarzania danych osobowych

Polityka bezpieczeństwa

Instrukcja zarządzania systemem informatycznym

www.giodo.gov.pl

POLITYKA BEZPIECZEŃSTWA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Polityka bezpieczeństwa powinna zawierać (§ 4 rozporządzenia)

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

INSTRUKCJA ZARZĄDZANIA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

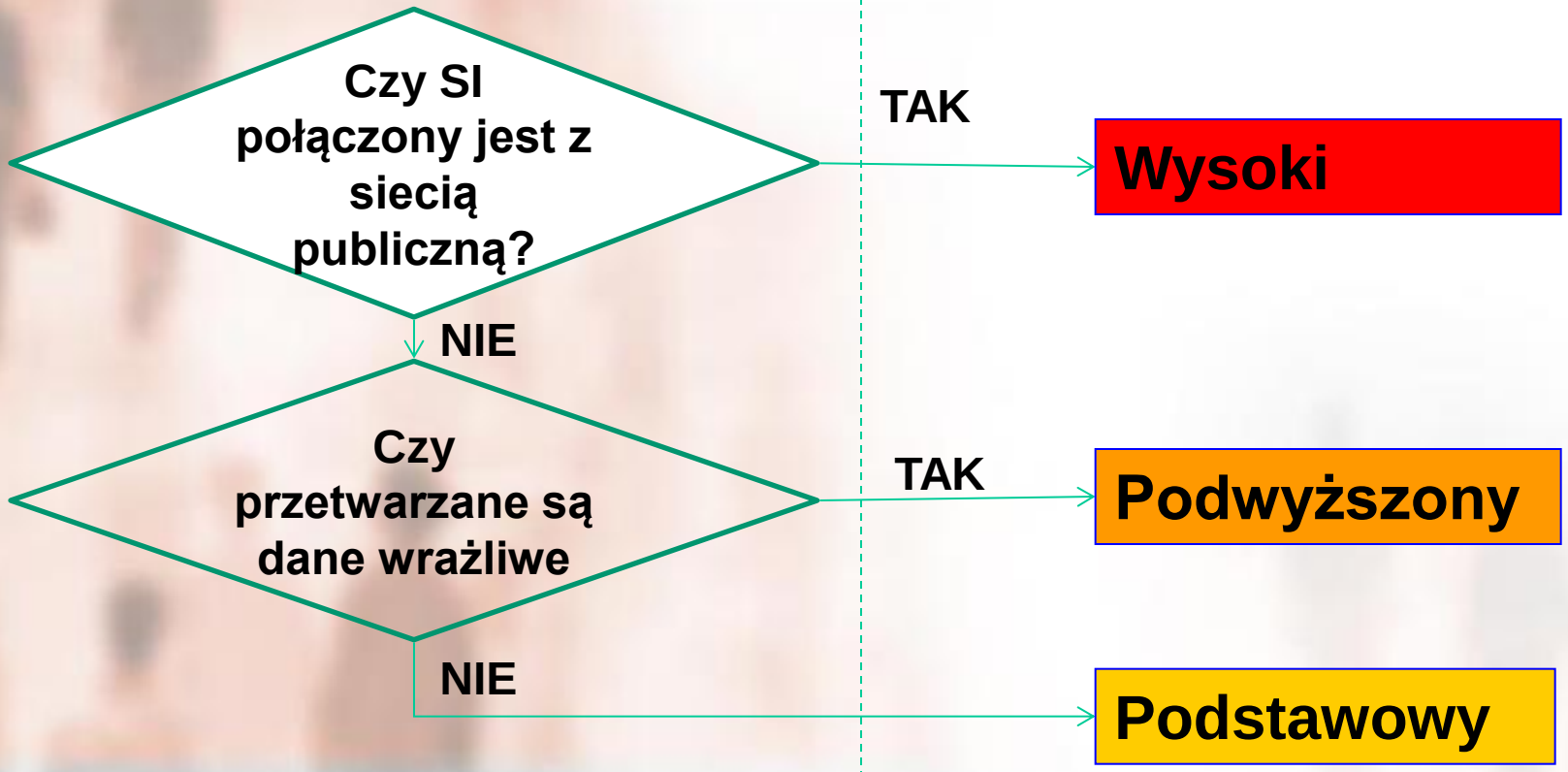
Instrukcja zarządzania SI powinna zawierać (§ 5 rozporządzenia)

1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
2) stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
4) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
5) sposób, miejsce i okres przechowywania kopii zapasowych:
6) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego;
7) Sposób realizacji odnotowań o udostępnieniach danych;
8) Procedury wykonywania przeglądów, napraw, likwidacji sprzętu

POLITYKA BEZPIECZEŃSTWA
POZIOMY BEZPIECZEŃSTWA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Poziom zagrożeń, Kategorie danych	Wymagany poziom bezpieczeństwa



Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

www.giodo.gov.pl

WYMAGANIA BEZPIECZEŃSTWA
Rozporzadzenie

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Minimalne wymagania ochrony (załącznik do rozporządzenia)

Podstawowy

1) Zabezpieczenie obszaru przetwarzania;
2) Kontrola dostępu (indywidualne konto dla każdego użytkownika);
3) Zabezpieczenie przed szkodliwym oprogramowaniem i awarią zasilania;
4) Niepowtarzalność identyfikatora, odpowiednie parametry dotyczące hasła oraz obowiązek tworzenia kopi zapasowych;
5) Kryptograficzne zabezpieczenie komputerów przenośnych;
6) Odpowiednie procedury przenoszenia, likwidacji i napraw sprzętu;
7) Monitorowanie wdrożonych zabezpieczeń;

Podwyższony

8) Dodatkowa wymagania parametrów hasła dla danych wrażliwych;
9) Dodatkowe zabezpieczenie danych wrażliwych opuszczających obszar przetwarzania (ochrona kryptograficzna);
10) Opis sposobu zabezpieczenia o którym mowa w punkcie 9 i jego ochrona;

Wysoki

11) Kontrola i zabezpieczenie przepływy danych na styku z siecią publiczną;
12) Kryptograficzna ochrona danych przesyłanych w sieci publicznej;

www.giodo.gov.pl

BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Zarządzanie bezpieczeństwem informacji (ZBI) jest dziedziną interdyscyplinarna z pogranicza techniki, organizacji i prawa.
2. ZBI ma własna ciągle rozwijająca się terminologię i metodykę.
3. Kluczowymi pojęciami z obszaru ZBI są pojęcia: zasoby (aktywa), zagrożenia, podatności, następstwa, ryzyka.
4. ZBI wykorzystuje szereg modeli. Kluczowym modelem jest model związków pomiędzy elementami bezpieczeństwa oraz model związków w zarządzaniu ryzykiem.
5. ZBI w instytucji. Trójpoziomowy model hierarchii celów, strategii i polityk bezpieczeństwa.

I. Bezpieczeństwo instytucji
II. Bezpieczeństwo systemów informatycznych w instytucji
III. Bezpieczeństwo konkretnego systemu (serwera, klientów, łączności)

www.giodo.gov.pl

BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo informacji: zachowanie poufności, integralności i dostępności informacji: PN-ISO/IEC 27000

Poufność–zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym

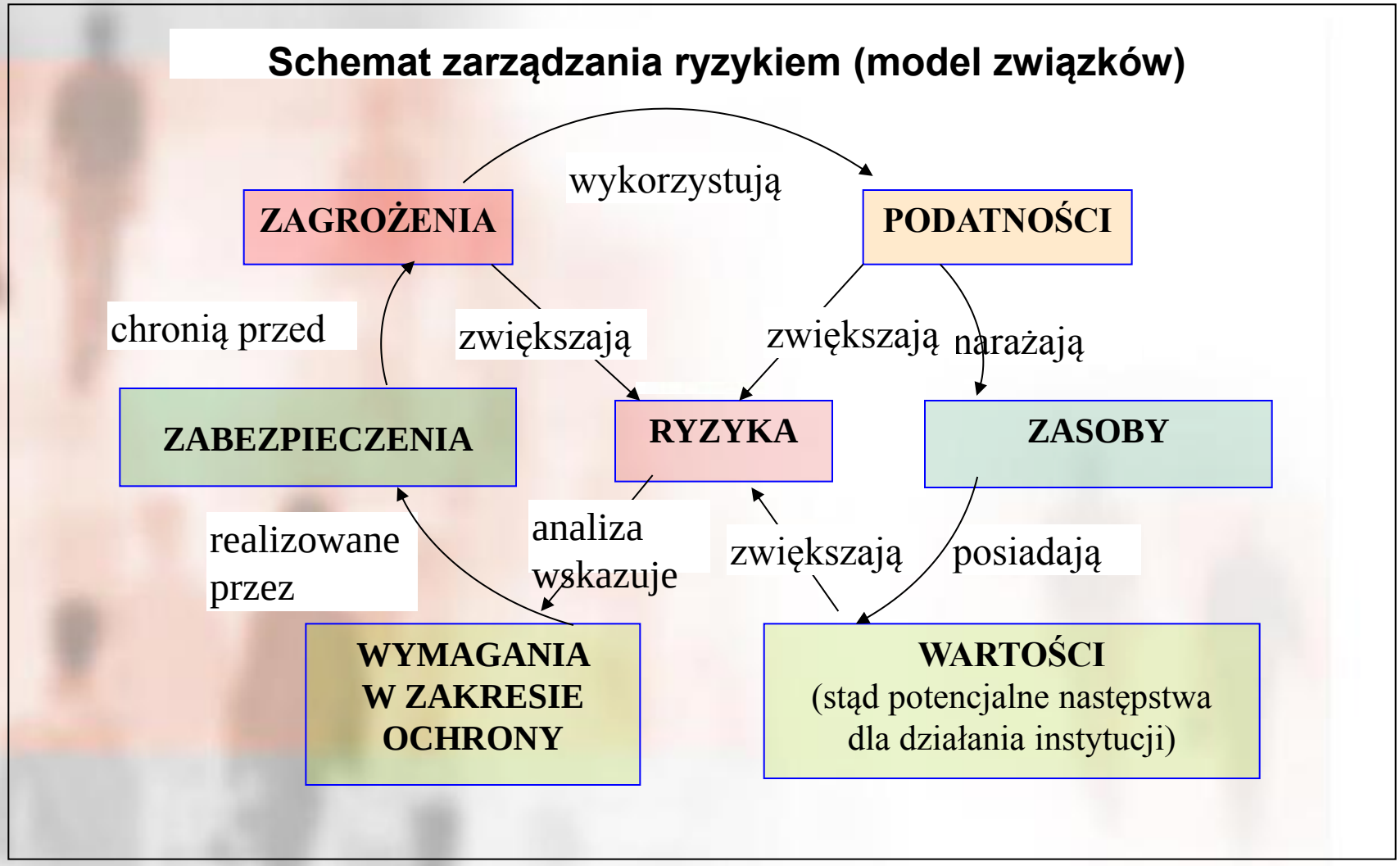
Integralność–zapewnienie dokładności i kompletności informacji oraz metod przetwarzania

Dostępność-zapewnienie ze osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy gdy jest to potrzebne

www.giodo.gov.pl

BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (3)

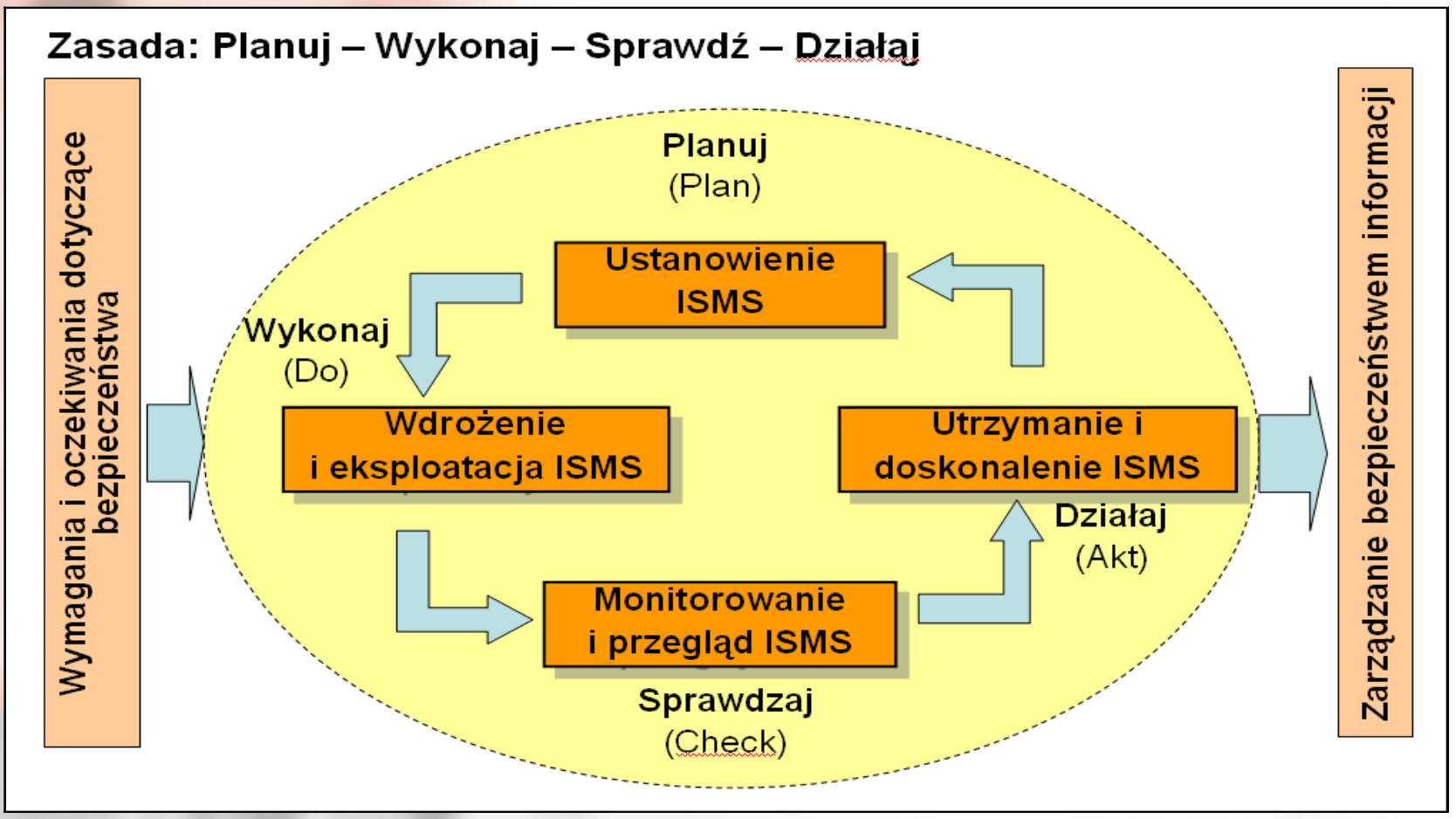
GIODO
Generalny Inspektor Ochrony Danych Osobowych



BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

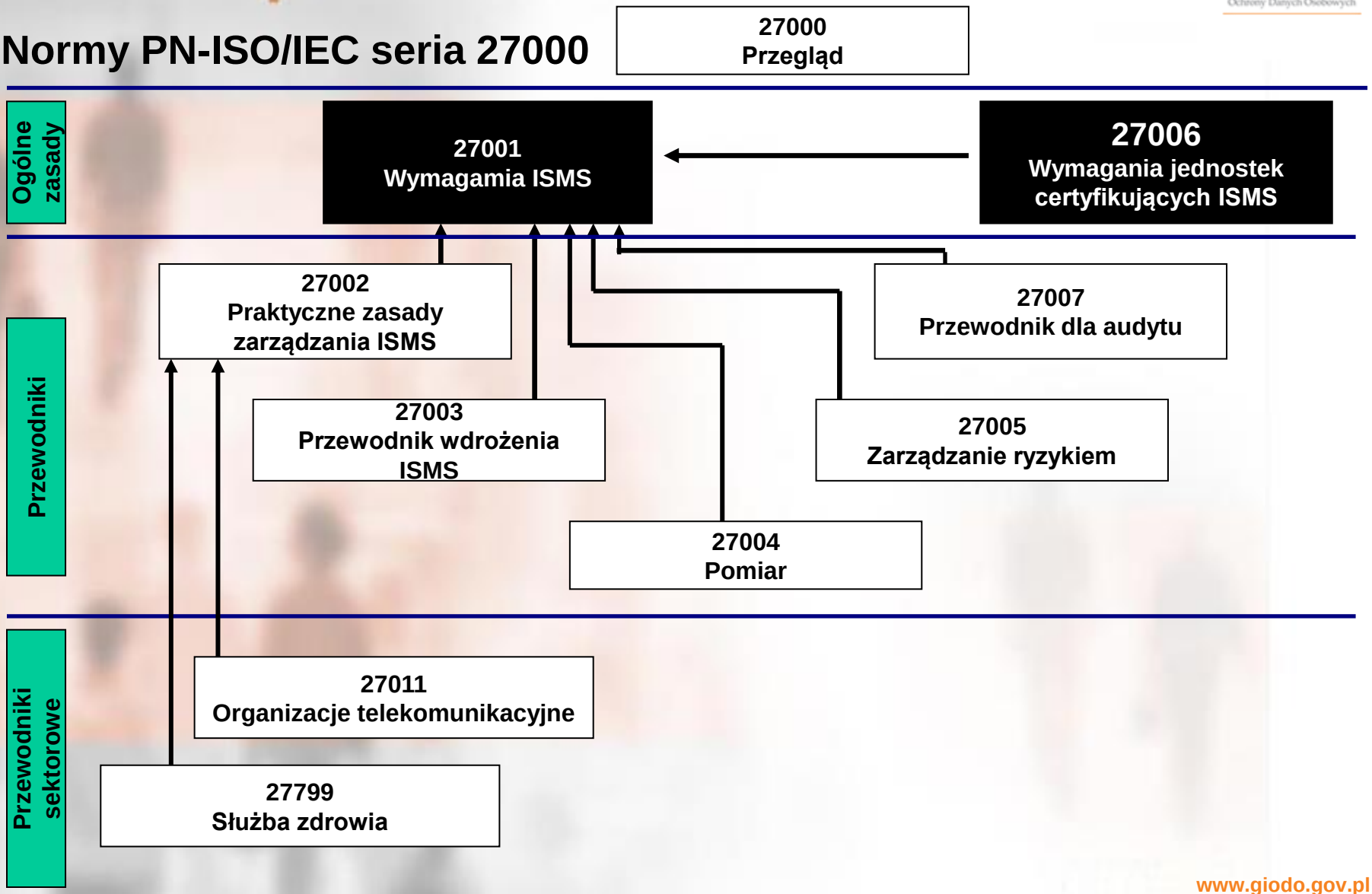
Zarządzanie bezpieczeństwem



BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (5)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Normy PN-ISO/IEC seria 27000



www.giodo.gov.pl

NORMY A PRZEPISY PORAWA

GIODO
Generalny Inspektor Ochrony Danych Osobowych

NORMALIZACJA

LEGISLACJA

NORMY

- opracowywane przez zainteresowane strony w ramach jednostki normalizacyjnej
- mają status zaleceń

PRZEPISY TECHNICZNE

- przyjmowane przez prawodawcze organy państwa
- stanowią obowiązek prawny dla obywateli

www.giodo.gov.pl

GIODO
Generalny Inspektor Ochrony Danych Osobowych

POWOŁYWANIE SIĘ NA NORMY W PRZEPISACH

Powołanie w sposób wyłączny, z którego wynika, że jedynym sposobem spełnienia wymagań przepisu jest zgodność z normami na które się powołano

Powołanie wskazujące, z którego wynika, że jednym z możliwych sposobów spełnienia wymagań przepisu prawnego jest osiągnięcie zgodności z normami na które się powołano *(np. koncepcja norm zharmonizowanych z Dyrektywami Nowego Podejścia)*

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Rozdział IV. § 15

1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: **PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.**

www.giodo.gov.pl

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV. § 16

1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku gdy w danej sprawie brak jest przepisów, norm lub standardów, o których mowa w ust. 1, stosuje się standardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:
   1) **Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),**
   2) **World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)**

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV.

§ 19. W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań **Web Content Accessibility Guidelines (WCAG 2.0)**, z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

§ 20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (5)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;

6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;

7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (6)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;

11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (7)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2. Wymagane działania: c.d.

12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:

a) dbałości o aktualizację oprogramowania,

b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,

c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,

d) stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych.

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH (8)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI, ……

Rozdział IV. § 20. 2 Wymagane działania: c.d.

13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjecie działań korygujących;

14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Rozdział IV. § 20. 3

Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy **PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:. **1) PN-ISO/IEC 17799, 2) PN-ISO/IEC 27005, 3) PN-ISO/IEC 24762**

PRAKTYCZNE ASPEKTY BEZPIECZEŃSDTWA WG ISO/IEC 17799

GIODO
Generalny Inspektor Ochrony Danych Osobowych

12. Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

- Wymagania bezpieczeństwa systemów informacyjnych
- Poprawne przetwarzanie w aplikacjach
- **Zabezpieczenia kryptograficzne**
- Bezpieczeństwo plików systemowych
- **Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej**
- **Zarządzanie podatnościami technicznymi**

Polityka korzystania z zabezpieczeń kryptograficznych

Zarządzanie kluczami

Procedury kontroli zmian

Techniczny przegląd aplikacji po zmianach w systemie operacyjnym

Ograniczenia dotyczące zmian w pakietach oprogramowania

Wyciek informacji

Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej

Nadzór nad podatnościami technicznymi

Dostawcy są często pod znacznym naciskiem, aby wydawać poprawki tak szybko, jak to możliwe. Z tego powodu poprawka może nie rozwiązywać problemu w wystarczający sposób oraz może mieć negatywne skutki uboczne. Ponadto, w niektórych przypadkach, po zainstalowaniu poprawki jej odinstalowanie może być utrudnione

PRZYDATNA LITERATURA

1. Jerzy Krawiec, Artur Stefaniak, System Zarządzania Bezpieczeństwem Informacji w praktyce. Zasady wyboru zabezpieczeń, PKN, Warszawa 2011
2. Praca zbiorowa, Normalizacja, PKN Warszawa 2013
3. Praca zbiorowa, Ochrona danych osobowych w praktyce, PKN Warszawa 2013
4. PN-ISO/IEC 27001 Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji. Wymagania
5. PN-ISO/IEC 17799 Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji
6. PN-ISO/IEC 27005 Technika informatyczna - Techniki bezpieczeństwa - Zarządzanie ryzykiem w bezpieczeństwie informacji
7. PN-ISO/IEC 24762 Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie

Dziękuję za uwagę

Andrzej Kaczmarek

BIURO

GENERALNEGO INSPEKTORA OCHRONY

DANYCH OSOBOWYCH